Có một công cụ sẵn có mà gần như sẽ bảo đảm rằng không ai có thể đọc được nội dung thư từ và những dữ liệu khác mà bạn gửi trực tuyến. Công cụ này được gọi là PGP.
PGP là từ viết tắt của “Pretty Good Privacy.” Nó cho phép người gửi và người nhận email và tài liệu một cách an toàn.
Do cấu trúc phân cấp của Internet, những kẻ xấu có thể xem được những thư từ tin nhắn khi chúng lưu thông trên mạng
Để giúp bảo vệ thông tin liên lạc, PGP dựa trên một tập hợp ba loại khóa để mã hóa và giải mã thông điệp.
Công khai
Mã hóa một thông điệp mà chỉ có khóa riêng tư tương ứng mới có thể giải mã được
Kẻ xấu vẫn có thể chặn giữ trao đổi liên lạc, nhưng không có khóa riêng tư thì sẽ không thể giải mã được.
PGP lần đầu tiên được tạo ra vào đầu những năm 1990 bởi kỹ sư tiên phong Phil Zimmermann và kể từ đó đã có một số cập nhật và bổ sung lớn. PGP thực tế là một chương trình mã hóa rất mạnh mẽ.
Khi một cái gì đó được “mã hóa,” về cơ bản nó được chuyển đổi từ văn bản bình thường thành một mật mã mà lý tưởng thì chỉ có thể giải mã được nhờ sự trợ giúp của một khóa điện tử. Bất cứ ai nhận được thông điệp được mã hóa mà không có khóa bí mật sẽ chỉ nhìn thấy ký tự vô nghĩa và sẽ phải tìm cách giải mã. Khóa càng phức tạp thì càng khó giải mã.
PGP có thể mã hóa email, văn bản, tài liệu hoặc thậm chí toàn bộ bộ nhớ của máy tính thông qua một sự kết hợp những thủ thuật mã hóa rất mạnh. Một khi được mã hóa bằng PGP, người dùng cảm thấy khá yên tâm rằng hầu như không ai – ngay cả đến những người giải mã phức tạp nhất ở bất cứ nơi đâu trên thế giới – sẽ có thể giải mã và do thám xem người dùng đang làm gì.

Cách thức hoạt động
Bất kỳ công cụ mạnh mẽ nào như PGP đều có những phức tạp và rắc rối. Ít người sử dụng PGP thực sự hiểu được những thuật toán mã hóa phức tạp và những bước được sử dụng, nhưng những khái niệm về cách sử dụng PGP khá cơ bản.
Thay vì chỉ sử dụng một khóa, PGP sử dụng một số khóa mã điện tử: một khóa công khai, một khóa riêng tư, và một khóa chỉ dùng cho phiên làm việc.
Khóa công khai được chia sẻ rộng rãi cho tất cả mọi người dùng PGP và được sử dụng để mã hóa tài liệu. Khóa riêng tư chỉ dành cho người dùng cá nhân để giải mã dữ liệu được gửi cho họ thông qua khóa công khai của mình. Cuối cùng, khóa phiên là duy nhất cho mỗi hành động mã hóa.
Nó hoạt động như sau. Một trong những điều đầu tiên mà người mới dùng PGP làm là tạo khóa công khai và riêng tư của mình. Đó là những chuỗi dài những ký tự điện tử có vẻ như vô nghĩa. Độ dài của khóa có thể khác nhau tùy thuộc vào mức độ mã hóa mà người dùng muốn sử

dụng, nhưng sự khác biệt giữa khóa công khai và riêng tư là tối quan trọng.
Người dùng PGP được khuyến khích chia sẻ khóa công khai của mình ở bất cứ nơi nào họ muốn: đó là thứ mà những người dùng PGP khác sẽ cần khi họ gửi một thông điệp mã hóa hoặc tài liệu cho bạn. Khóa riêng tư nhất thiết phải mang tính riêng tư: chỉ dành cho người dùng và không bao giờ chia sẻ với ai. Khóa riêng tư cũng phải được bảo vệ, bởi vì nếu bạn làm mất khóa riêng tư của mình thì kể như bạn mất luôn và bất kỳ tài liệu nào được mã hóa bằng khóa riêng tư sẽ bị mất.
Một khi bạn có email hay tài liệu muốn mã hóa, và khóa công khai của người mà bạn muốn gửi tới, người dùng sẽ “ký tên” hay mã hóa văn bản của mình bằng cách sử dụng thứ được gọi là “cụm từ mật khẩu PGP” và gửi đến cho người nhận.
Khi văn bản đến đúng người nhận, nó sẽ trông giống như một mớ ký tự vô nghĩa, nhưng người nhận – sử dụng khóa riêng tư của họ và mật khẩu độc nhất – sẽ có thể giải mã được văn bản mà không ai khác làm được do thông tin về khóa được gói bằng mã hóa. Quá trình hoạt động diễn ra y hệt theo chiều ngược lại. Giống như khóa những thông điệp trong hai cái hộp mà chỉ có người gửi và người nhận mới có thể mở khóa.
Dù đang có tranh luận ở những cấp cao nhất trong lĩnh vực mã hóa rằng liệu có một hệ thống mã hóa kỹ thuật số nào đó thực sự “không thể giải mã được” hay không, song có sự đồng thuận rộng khắp rằng PGP cung cấp điều gần nhất với việc bảo đảm thông tin liên lạc thực sự riêng tư. Ở những thiết định riêng tư cao nhất, gần như không tài nào mở khóa được những tài liệu mã hóa bằng PGP mà không có sự trợ giúp của siêu máy tính và một đội ngũ những người giải mã tài năng … và thậm chí có thể còn không giải mã nổi. Nếu bạn có những tài liệu mà bạn muốn bảo đảm không ai ngoài bạn sẽ thấy, hoặc cần sự bảo đảm nghiêm ngặt để những trao đổi liên lạc bằng email của bạn vẫn giữ được tính riêng tư, không có thứ gì có thể qua được PGP.
Nhược điểm khả dĩ
Nhưng có một số nhược điểm.
Thứ nhất, dù PGP gần như bảo đảm được tính riêng tư của những tài liệu được mã hóa, nó không làm gì để bảo vệ danh tính của cả người gửi và người nhận. Nó chỉ là một công cụ mã hóa không hơn, thậm chí khi sử dụng nó hoạt động trực tuyến của bạn cũng lộ rõ hệt như khi bạn không sử dụng nó. Điều đó có nghĩa là chính quyền sẽ không biết bạn nói gì trên mạng, nhưng họ sẽ biết bạn nói với ai. Ngoài ra, PGP là một công cụ phức tạp. Ngay cả những người dùng có kinh nghiệm thường phải cân nhắc những bước chính xác trong việc mã hóa và giải mã. Những người có thể tự coi mình là chưa rành về Web nên suy nghĩ thật kỹ về việc dùng PGP.
Tóm lại
Nếu bạn cần gửi hoặc lưu trữ tài liệu một cách an toàn mà không sợ có thể bị chặn đọc, và bạn chịu khó vượt qua một số bước phức tạp để thực hiện, PGP là công cụ dành cho bạn. Nếu bạn muốn phần mềm giúp bạn vượt tường lửa Internet hay bảo vệ sự riêng tư của bạn trên mạng, hay bạn dễ nản lòng vì phần mềm phức tạp, PGP không giúp bạn được nhiều.